Information Security Service Provider Risk Assessment Questionnaire

Ministry of Central Services
Information Technology Division
Information Security Branch

Last revised: August 2018
Last reviewed: October 2018
Next review: October 2018

Table of Contents

Revision History

Date (dd/mm/yyyy)	**Version**	**Comments**	**Reviewers Name**
06/06/2018	0.1	Created document based on new templates	Darren Sproat
09/08/2018	0.2	Added question about evaluation of solutions against Protection Profile for Common Criteria.	Darren Sproat
02/10/2018	0.3	Reviewed for accuracy – No revisions at this time.	Darren Sproat

Overview

This questionnaire is provided to Service Provider who deliver or intend to deliver IT Solutions and/or Services to the Government of Saskatchewan. It is intended to assist with the assessment of a Service Provider's information security posture and maturity and informs GoS activities including, though not limited to, Threat and Risk Assessments and Privacy Impact Assessments. Service Providers are asked to provide responses to each question and email the completed questionnaire to the GoS ITO Information Security Branch at ITOInformationSecurityBranch@gov.sk.ca.

NOTE: The Government of Saskatchewan acknowledges that not all questions will be applicable to every service or solution delivery engagement. If, in your determination, a question is not applicable, indicate as such with an explanation as to why it is not applicable.

Service Provider Information

1. Provide full Service Provider contact information including service provider name, full address, contact name, telephone number, and email address. Include this information for any and all service providers who will take part in the delivery of the solution and/or services to the Government of Saskatchewan.

Solution or Service Agreement

With every engagement, contractual documents mutually agreed upon between the Service Provider and the Government of Saskatchewan are expected. Such documents may include, though are not necessarily limited to master agreements, service agreements, software licensing agreements, statements of work, security documents, service level agreements, or other documents describing the specifics of the relationship between the service provider and the Government of Saskatchewan and the Service Provider. The following questions apply if there will be contractual documents provided by the Service Provider (in place of or in addition to documents provided by the Government of Saskatchewan).

2. Will a formal Service Provider agreement be used to define the relationship and the service and/or solution delivery engagement?

3. Does the agreement, described in response to question 2, contain clauses addressing security? Common examples are listed below. In response to this question, identify, to the best of your knowledge and ability, which documents will address each of the following example clauses.

    - Non-disclosure of Government of Saskatchewan information;
    - Designating mutual security contacts;
    - Reporting of security breaches or incidents to the Government of Saskatchewan;
    - Use of a secure development environment;
    - Protection of test data;
    - Screening requirements for Service Provider personnel;
    - Right to audit Service Provider processes and controls;
    - Defect resolution and conflict resolution processes;
    - Service Provider obligation to deliver periodic independent reports on effectiveness of controls;
    - Ensuring effective security in the Service Provider supply chain;
    - Continuity assurance in the event the Service Provider becomes unable to supply its products or services;
    - Disposition of Government of Saskatchewan data at termination or expiry of the service or solution delivery engagement.

Security Program

4. Does the Service Provider have a written information security policy? If yes, append a copy of the information security policy. If not, explain.

5. Does the Service Provider have a copy of GOS's information security policy and are they willing to comply with the policy as well as the data protection standards within?

6. Does the Service Provider have a single point of contact for security-related concerns for the Government of Saskatchewan? If so, provide the single point of contact. If not, explain. NOTE: If the single point of contact is an individual, a backup or escalation point should also be provided.

7. Has the Service Provider achieved a recognized information security standard such as ISO/IEC 27001:2013? If so, what is that standard and does the Service Provider's entire business (or proposed Services/Solutions) fall within the scope of that standard? If not, explain.

8. Has the Service Provider implemented an IT Governance framework such as ITIL or ISO 27001? If so, describe the framework and the standard to which it aligns. If not, explain.

9. Will the Service Provider be processing credit cards on behalf of the Government of Saskatchewan? If yes, is the Service Provider (and its proposed Services/Solutions) PCI DSS compliant?

10. Does the Service Provider have a formal change control process for IT changes and are information security implications a formalized part of change control and review? If so, describe the process. If not, explain.

11. Does the Service Provider have a dedicated security team or resource(s) with information security duties? If so, describe. If not, explain.

12. Do the Service Provider's employees receive information security awareness training? If so, describe this awareness training. If not, explain.

13. Is a background check required for all Service Provider employees and contractors accessing and handling the organization's data?

14. Does the Service Provider have security measures in place for protecting confidential information? If so, describe in detail. If not, explain.

15. Has the Service Provider's proposed solution been evaluated against Protection Profile for Common Criteria (ISO/IEC 15408) or a similar industry certification or information security evaluation standard? If so, describe. If not, explain.

Technological Security Measures

16. Are Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS) used by the Service Provider? If yes, provide a network topology for the environments illustrating location of these components and other supporting elements of the infrastructure.

17. Is antivirus software installed and maintained on data processing servers?

18. Is antivirus software installed and maintained on workstations?

19. Are system, application, and security patches applied to workstations and servers on a routine basis within a formal patch management process? If so, provide details of the process. If not, explain.

Access Control

20. Do the Service Provider's employees and contractors have a unique log-in IDs when accessing data?

21. Is access restricted on systems that contain sensitive data? If yes, what controls are currently in place to restrict access? If not, explain.

22. Is there formal control of access to System Administrator privileges? If so, describe the controls in place. If not, explain.

23. Are the Service Provider's employees and contractors required to use a VPN when accessing systems from all remote locations?

24. Does the Service Provider allow wireless access? If yes, describe how wireless access is protected.

25. Is physical access to data processing equipment (servers and network equipment) restricted? If yes, what controls are currently in place?

26. Are network boundaries protected by firewalls?

27. Will the Government of Saskatchewan be permitted access to supported environments to perform penetration testing, threat and risk assessments, and other assessments/audits? If so, what level of access will the Government of Saskatchewan have? If not, explain.

Testing and Compliance

28. Are servers configured to capture who accessed a system and what changes were made? If not, in case of a security breach or incident, how does the Service Provider determine who accessed the system and what changes were made?

29. Are system and security patches tested prior to implementation in the production environment?

30. Is regular network vulnerability scanning performed? If so, describe the frequency and/or process related to vulnerability analysis. If not, explain.

31. Does the Service Provider receive a CSAE-3416 or equivalent report? If so, provide a copy of the latest report.

Continuity

32. Does the Service Provider outsource its data storage? If yes, to who is the data outsourced and what measures/controls are in place to ensure data continuity and protection?

33. Are computer systems (servers) backed up according to a regular schedule? If so, describe the backup process/schedule. If not, explain.

34. How does the Service Provider verify back-up and recovery processes?

35. Does the Service Provider store backup's offsite?

36. Does the Service Provider encrypt its backups?

37. What processes and/or policies apply upon end-of-contract for transition of Solution and Services; particularly, Government of Saskatchewan data?

Security Incident Management

38. Does the Service Provider have a formal Incident Response plan? If so, describe how the Service Provider handles data incidents such as breaches or other information security incidents. If not, explain.

39. If an information security breach involving Government of Saskatchewan data occurred, would the Government of Saskatchewan be notified of the breach? If yes, how soon would the notification be made? If not, explain.